# Security Measures And Controls

IRIS Connect takes the responsibility of acting as a processor of personal data extremely seriously.  We constantly review our procedural, organisational and physical security to ensure that we are offering a service that our customers can trust.

We have completed multiple external audits, gap analysis and penetration testing of our services to ensure that we meet industry best practices and the principles of GDPR.

All data is stored and processed on Amazon Web Services (AWS) infrastructure.
The data is restricted to centres based in:

- Ireland for our EU platform
- America for our US platform
- Australia for our OCE platform

AWS are international industry leaders in the provision of secure cloud services and they hold numerous domestic and international security accreditations.

Please visit this page for further information on Amazon security and compliance.

In addition to their international reputation and security and compliance certifications, we have had confidential access to their independent SOC-2 audit report so that we could review and analyse their security in detail.

## 1. Physical security of data

The AWS environment utilises state-of-the art network security, electronic surveillance, physical security and multi-factor access control system to protect client data. The data centres are staffed 24×7 by trained security teams.

## 2. Storage redundancy

To enhance redundancy we:

- Take hourly backups of our database
- Save data to multiple availability zones within the region.
- Verify the integrity of the data using checksums, automatically repairing any data inconsistencies

## 3. Destruction of data

Customer data (financial) is retained in line with local legal frameworks.

Customer data (non-financial) will be securely disposed of and / or transferred to the client following termination of licence.

Data that the client has deleted will be held in a deleted state for 90 days, then deleted completely. 180 days later, the last backup dataset that contained the resource will be deleted. The time period from user deletion to complete removal is 270 days (approx nine months).

There are certain occasions when information needs to be preserved beyond this limit, such as in the following circumstances:

- Legal proceedings or a regulatory or similar investigation or obligation to produce information are known to be likely, threatened or actual
- A crime is suspected or detected

The highest standard of industry procedure is used when decommissioning of storage devices at the end of their useful life.

## 4. Secure encryption

IRIS Connect ensures any data in transit is encrypted using the leading industry practice (TLS 1.2 ). Data at rest is encrypted with 256-bit Advanced Encryption Standard (AES-256). Additionally, data stored on mobile devices is encrypted to ensure that it is protected before it enters our secure cloud services.

## 5. Organisational security

IRIS Connect, in line with GDPR and ISO27001 recommendations, regularly reviews its organisational and cyber security and has comprehensive information security processes and protocols.

We have been externally audited and certificated to ensure that we comply to a high standard of organisational and cyber security.

## 6. Service level

IRIS Connect utilises market leading services for data processing and storage. We use automatically scaling infrastructure to deal with increases in service traffic.

IRIS Connect have provided 99.9% service uptime in the last 18 months during core operating hours (8am – 6pm).

IRIS Connect provides free full support to all customers, enabling us to quickly resolve any issues logged. This is provided Monday – Friday between 8am – 5.30pm GMT, with additional limited support until 10pm.

The support team is available via live chat, email and phone.

## 7. Authorization and access control

IRIS Connect has been constructed with privacy-by-design principles at its core.  This ensures that user role separation and permissioning governs access to appropriate data and features.

Each IRIS Connect client nominates an Organisation Administrator who is responsible for agreeing to and enforcing the IRIS Connect End User Licence Agreement (EULA) when they first sign into the system.

The terms of the EULA make the use of the system conditional on appropriate local agreements to ensure that all relevant parties are informed about the use of the system and have provided appropriate permissions for the capture and sharing of video.

The EULA also stipulates that the system is used within a supportive developmental framework and that end users are aware of their obligations and responsibilities for data management and sharing. This agreement also gives individual users the right to delete videos and ensures that individual videos will not be recorded or shared with any other IRIS Connect user without their
explicit permission.

The IRIS Connect system is based on individual user accounts and permissioning. This means that the observed user has to agree to a recording taking place before the system allows another user to connect to the camera. The same protections exist once a video has been encrypted and uploaded. This means users are only able to see data that has been explicitly shared with them. By default users are limited to sharing videos with other users at their organization, although collaboration with other organizations can be enabled at the request of the clients' Organization Administrator who has appropriate data sharing agreements in place.

Users have complete control over who has access to their data by deciding to share videos either with individual users or into a group library. A fundamental principle of the system is that users will never "lose sight or control" of their video. They will always be able to see the video and any associated data.

Users retain the right to delete a video or remove sharing privileges at any time.

Our staff have strict controls over who may access data and protocols for gaining permission from clients if access is required.

## 8. Input data that contain personal data

Only the data owners have access to the data at the input stage. Users are responsible for input into the system, and data can only be input into users' specific account with the confidential password and unique username.

IRIS Connect Equipment, including the LiveView UploadBox, Apple & Android devices (when used with the IRIS Connect app) do not permanently store files locally.

For full user control and data security, videos are never stored on individual devices or local servers. Instead, they are encrypted, immediately uploaded to our platform and automatically deleted from the device they were recorded on. The platform is designed to ensure that data remains in the secure, password protected environment.

The deletion of the input data by a user is managed via an automated process build into the design of the system

## 9. Output data that contain personal data

The IRIS Connect system is based on individual user accounts and permissioning, where each user has their own personal username and password for their account in our platform. The observed user has to agree to a recording taking place before the system allows another user to connect to the camera. The same protections exist once a video has been encrypted and uploaded. This means users are only able to see data that has been explicitly shared with them. Users are limited to sharing videos with other users at their organisation, or collaboration with other organisations if this has been enabled with the permission of the Organisation Administrator.

All data is securely stored and can only be delivered to the user via an encrypted channel.

The organisation and its users are in complete control of their data, so we will only destroy data upon the instruction of the Data Controller. If the data is deleted by the owner, deleted

data will be stored for 3 months in case the customer needs to retrieve it. The back-ups will be stored for a further 3 months before being securely and automatically destroyed to ensure that it cannot be misused or accessed by unauthorised persons

## 10. External communication connections

The IRIS Connect system is fully cloud-based and designed to ensure that unauthorised persons cannot gain access to data. IRIS Connect ensures any data in transit is encrypted using the leading industry practice (TLS 1.2). Any data removed from our secure system is done so under authorisation of the Data Controller or by authorised personnel for the purpose of data processing.

## 11. Control of rejected access attempts

The IRIS Connect platform logs every account login attempt. The system also blocks repeated login attempts to the same account within a determined time period, by locking the user’s account until this is reviewed by an authorised person.

## 12. Logging

IRIS Connect collects comprehensive user activity logs that are stored for six months.

## 13. Home offices

IRIS Connect does not permit and physically restrict data processing at home including holding data locally, or printing data locally. All data is held securely within our cloud-based system.

## 14. GDPR Security obligations

IRIS Connect has completed an external audit of all of its services and teams to ensure that it is fully compliant with GDPR, including article 32.

## 15. Privacy by design

As recommended by the ICO, IRIS Connect has been constructed with privacy-by-design principles at its core. This ensures that user role separation and permissioning governs access to appropriate data and features. Each IRIS Connect client is required to nominate

an Organisation Administrator and Data Protection Officer who are responsible for agreeing to, and enforcing, the IRIS Connect terms and conditions for use.
These terms make the use of the system conditional on appropriate local agreements to ensure that all relevant parties are informed about the use of the system and have provided appropriate permissions for the capture and sharing of video.

By default, users are limited to sharing videos with other users at their organisation, although collaboration with other organisations can be enabled by the Organisation Administrator where they have appropriate data sharing agreements in place. There are automated systems and interfaces in place that allow Organisation Administrators to quickly increase or decrease the scope in which their users can share data.

Users have complete control over who has access to their data, within the scope defined by the Organisation Administrator, deciding to share observations either with individual users or into a group library. A fundamental principle of the system is that users will never “lose sight or control” of their video. They will always be able to see the video and any associated data. Users have the ability to delete a video or remove sharing privileges at any time.

Only the data owners have access to the data at input stage. Users are responsible for input into the system, and data can only be inputted into users specific accounts with the confidential password and unique username. The deletion of the inputted data by a user is managed via an automated process built into the design of the system. All data is securely stored and can only be delivered to appropriate users via an encrypted channel

## 16. External review, certification and audit

We have been externally audited and certificated to ensure that we comply to a high standard of organisational and cyber security. This includes:

- Achieved Department for Education’s Cloud Service Providers Self Certification which was independently verified
- Gained Government-backed industry supported scheme; Cyber Essentials
- ISO and GDPR gap analysis via an independent 3rd party auditor

# 17. Additional security controls

In line with GDPR, IRIS Connect are able to provide the additional security controls:

**Password Security:** An organisation is able to configure the password required strength (length and complexity) for users' accounts for the IRIS Connect platform.  This can be customised to either medium or high requirements depending on the organisation's need. To request this feature contact our support desk.

**Anonymisation of shared data:** The owner of any video on the IRIS Connect platform can automatically convert their video to anonymised mode prior to sharing.
*Use Case*: This tool preserves the anonymity of learners by obscuring distinguishing features, assuming that no other identifiable details are contained in the video (such as someone using a data subject's full name within the clip) this enables broader sharing of video assets. Further information about this feature can be found in our help guides.

**Mobile app auto-anonymisation of recordings**: Either the individual user or the Organisation Administrator can set recordings with the Record app to be recorded  using the anonymisation filter. This means no un-anonymised data is captured.

Version 0.3
Updated: April 2021